

UNIVERSIDADE TÉCNICA DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

Tecnologias de Redes de Comunicações

1º Trabalho de Laboratório

**Estabelecimento e caracterização
de um canal PPP**

Fernando Mira da Silva

SETEMBRO DE 2007

1 Objectivos

Pretende-se neste trabalho estudar o protocolo PPP (*Point to Point Protocol*), implementando para este efeito uma ligação série entre duas máquinas Linux. Numa segunda fase, será analisada uma forma simples de implementar um túnel VPN usando uma ligação PPP sobre uma ligação SSH entre dois pontos remotos. Finalmente, pretende-se que sejam realizadas medidas que permitam caracterizar do ponto de vista de tráfego a ligação PPP assim estabelecida e, em particular, o *overhead* resultante do estabelecimento da ligação.

A realização deste trabalho terá lugar durante três semanas de laboratório, com início na semana de 1 de Outubro e final na semana de 15 a 19 de Outubro. A entrega do relatório deverá ter lugar uma semana após a conclusão do trabalho (ou seja, no dia 22 de Outubro para os alunos do turno de 2ª feira e dia 25 de Outubro para os alunos de 5ª feira).

2 Ligação PPP

Para teste inicial do protocolo PPP, será usado a montagem apresentada na figura 1.



Figura 1 – Ligação de duas máquinas usando uma linha série

Para este efeito, cada grupo dispõe de duas máquinas de laboratório e de um cabo série. Uma máquina (designada Linux 2) será ligada à Internet através da rede geral do Tagus Park. A máquina Linux 1 estará ligada apenas à máquina Linux 2 através de um cabo série, fornecido no laboratório. Pretende-se estabelecer uma ligação à Internet da máquina Linux 1 usando a ligação série PPP com máquina Linux 2 e usando esta última como um encaminhador de acesso à rede.

1. Ligue a máquina Linux 2 à rede geral do IST/Tagus.
2. Defina os endereços IP a adoptar na ligação PPP.
3. Verifique quais os passos necessários para estabelecer a ligação PPP em Linux.
4. Estabeleça as opções necessárias no ficheiro `/etc/ppp/options` em ambas as máquinas para estabelecer uma ligação ppp de acordo com os parâmetros considerados. Use o modo debug e visualize as mensagens geradas durante o processo de ligação.
5. Analise o comportamento da ligação variando opções da ligação, nomeadamente o modo de autenticação, protocolo de *handshaking* e MRU.
6. Estabeleça as configurações necessárias para a máquina Linux 1 aceder de forma transparente à Internet. Teste a ligação.

No relatório deverão ser listadas as configurações realizadas para a plena funcionalidade da ligação e deverão ser mencionadas as opções PPP testadas e resultados obtidos.

3 Análise de desempenho de ligações IP

Numa rede para transmissão de dados em IP, o desempenho de protocolos em serviços com conexão, tais como o TCP, é afectado pelas características particulares da camada de ligação (*data-link layer*). A existência de congestão na rede podem accionar mecanismos de controle de congestão (redução do valor da *congestion window*), os quais por sua vez afectam a qualidade da ligação.

Para análise e teste de desempenho da ligação, existem várias ferramentas de análise, disponíveis para vários sistemas operativos.

- iperf <http://dast.nlanr.net/Projects/Iperf/>
- tcpdump <http://www.tcpdump.org/>
- tcptrace <http://www.tcptrace.org/index.html>
- Ethereal <http://www.ethereal.com/> ou
- Wireshark <http://www.wireshark.org/>

Para caracterizar uma ligação, é fundamental a análise, entre outros, dos seguintes parametros:

- RTT (*Round Trip Time*) e ritmo de perda de pacotes.

A realização destes valores pode ser realizada usando o comando *ping* e analisando a distribuição dos valores medidos (média e desvio padrão) para vários tamanhos de *payload* (6, 256, 512, 1024, 1460bytes).

- Medida da largura de banda e débito de desempenho em TCP

Para efectuar estas medidas, podem ser gerados fluxos TCP com a ferramenta *iperf*. A captura de pacotes pode ser efectuada com a ferramenta *tcpdump* e a análise de resultados através de ferramentas como o *tcptrace* ou o *xplot*. A captura dos pacotes pode ser efectuada com o *tcpdump*.

4 Análise da ligação série PPP

Usando as ferramentas referidas na secção 3, realize a análise do desempenho e de largura de banda efectiva do canal PPP sobre linha série. Relacione os resultados obtidos com o ritmo de transmissão disponível.

5 Realização de uma VPN com uma ligação PPP

Uma VPN (*Virtual Private Network* ou *Rede Privada Virtual*) permite a um utilizador remoto aceder a uma rede local protegida (a rede local a que se encontra institucionalmente ligado, designada no seguimento por rede de origem) através do estabelecimento de um canal de comunicação seguro (cifrado). Para além da segurança implícita da ligação, a VPN permite ao utilizador remoto ter acesso directo à sua rede local, obtendo nomeadamente localmente um endereço IP da sua rede de origem. Esta característica pode ser usada para, nomeadamente, permitir o acesso remoto a serviços protegidos e normalmente não acessíveis a utilizadores externos.

Embora existam diversas formas de realizar uma VPN, uma forma particularmente simples é realizar uma ligação ponto a ponto usando o protocolo PPP sobre uma ligação ssh. O ssh é uma forma simples de estabelecer uma comunicação segura entre um cliente e um servidor usando um canal cifrado e, embora habitualmente usada para o estabelecimento de uma sessão interactiva, permite outros tipos de comunicação. Em particular, é possível usar uma ligação PPP sobre este canal, conseguindo-se deste modo uma ligação equivalente à de uma VPN (ver figura 2).



Figura 2 – PPP sobre SSH

Pretende-se instalar um túnel de PPP sobre SSH. O servidor estará localizado numa máquina com sistema operativo Linux disponibilizada especificamente para este efeito no pólo da Alameda. O cliente será uma das máquinas Linux disponíveis no laboratório.

Cada grupo deverá:

1. Estabelecer os critérios
2. Estabelecer a ligação PPP sobre SSH para o servidor remoto e verificar o seu funcionamento. As credenciais de acesso este servidor serão dadas oportunamente.
3. Caracterizar a ligação (RTT e largura de banda disponível) entre uma máquina Linux local e o servidor, usando uma ligação IP directa com o servidor (ou seja, sem usar a ligação PPP sobre SSH).
4. Repetir os testes realizados no ponto 2 usando a VPN PPP sobre SSH criada e realizar uma análise comparativa dos resultados, comparando-os com os obtidos no ponto 3.

Nota: a análise realizada depende da largura de banda útil disponível entre o Tagus Park e a Alameda, a qual se encontra fortemente saturada durante grande parte do dia, mas que apresenta flutuações de débito elevadas. Deste modo, os alunos deverão tomar as precauções necessárias para garantir que os testes realizados nos pontos 2 e 3 são comparáveis e estatisticamente significativos.